

MULTIMEDIA



UNIVERSITY

STUDENT ID NO

--	--	--	--	--	--	--	--	--	--

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 2, 2015/2016

TAC 3121 – APPLIED CRYPTOGRAPHY (All sections / Groups)

04 March 2016
3.00p.m – 5.00p.m
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This question paper consists of 3 pages, including the cover page, with **SIX** questions only.
2. Attempt **FIVE** out of **SIX** questions. All questions carry equal marks and the distribution of the marks for each question is given.
3. Please print all your answers in the answer booklet provided.

Question 1

- (a) X.800 categorises security goals into *Confidentiality*, *Integrity*, *Availability*, *Authentication*, *Access Control* and *Non-Repudiation*. Identify and explain the goal(s) which cannot be achieved by Cryptographic techniques. [2 marks]
- (b)

S ₆	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

Figure 1. 6th Substitution-Box of DES

Referring to Figure 1, find the output of the 6th S-Box in DES given the input as:
011100 010001 011100 110010 111000 010101 110011 110000

[6 marks]

- (c) Secret key in Hill cipher is in the form of $n \times n$ matrix and the key is valid if the inverse of its determinant exists. How many determinants as such exist? [2 marks]

Question 2

- (a) Give the definitions and **ONE** example each for *security mechanism* and *security service*. [3 marks]
- (b) Compare and contrast *passive attack* and *active attack*. [3 marks]
- (c) One of the verification steps in DSS is to compute the component $w = s^{-1} \bmod q$. Show the steps of computing the multiplicative inverse w using the Fermet's Little Theorem. [4 marks]

Question 3

- (a) Decrypt the ciphertext using autokey cipher with key *easy*:
XHAQB ZIDCU KJXCI [4 marks]
- (b) Compare and contrast *monoalphabetic cipher* and *polyalphabetic cipher*. [4 marks]
- (c) 3DES has security level of 112 bits. If we encrypt a plaintext twice using two different keys with 3DES, will the security level be doubled up (224 bits)? Justify your answer. [2 marks]

Continued...

Question 4

RSA Parameters
 $p=7, q=17, e=11$

Figure 2. Parameters of a RSA encryption scheme

- (a) Explain why the value e is a valid RSA public key in the parameters of Figure 2? [3 marks]
- (b) Using parameters from Figure 2, calculate the private key d . [5 marks]
- (c) Decrypt the ciphertext $C=2$. [2 marks]

Question 5

- (a) Pseudorandom Number Generator (PRNG) such as SecureRandom in Java generates random numbers for cryptographic use. List down and explain any **TWO** constructions of PRNG. [4 marks]
- (b) Does any of Hash, MAC or digital signature provides the security goal of access control? Justify your answer. [2 marks]
- (c) Given the public keys of an ElGamal encryption scheme as $y=7$, $a=3$ and $q=37$, find out the private key x such that $y=a^x \bmod q$. [4 marks]

Question 6

- (a) Diffie-Hellman key exchanged is vulnerable to man-in-the-middle attack. Suggest a solution to this vulnerability and explain you answer. [3 marks]
- (b) What are the advantages and disadvantages of Browser Public Key Infrastructure trust model? [4 marks]
- (c) Consider a message to be signed is "*The secret to score an A in TAC3121 is to find the answers for all the tutorial questions*". Which digital signature scheme would you choose to sign on the message: FDH-RSA with 550-bit N or DSS with 550-bit p ? Justify your answer. [3 marks]

End of Page